ON THE SUPPLEMENT TO THE LAW OF
BIQUADRATIC RECIPROCITY

KENNETH S. WILLIAMS

ABSTRACT. A short proof is given of the supplement to the law of
biquadratic reciprocity proved by Eisenstein in 1844.

If \( \pi \) is a Gaussian prime, which is not an associate of \( 1 + i \), then
\( N(\pi) \equiv 1 \pmod{4} \) and the biquadratic residue character of the Gaussian
integer \( \alpha \) modulo \( \pi \) is defined by

\[
\left( \frac{\alpha}{\pi} \right)_4 = \begin{cases} 
0, & \text{if } \alpha \equiv 0 \pmod{\pi}, \\
(\pi^r), & \text{if } \alpha \not\equiv 0 \pmod{\pi} \text{ and } \alpha^{(N(\pi)-1)/4} \equiv i^r \pmod{\pi}, \\
& \text{with } r = 0, 1, 2, 3.
\end{cases}
\]

As Gaussian integers can be factored uniquely into primes, the Jacobi
extension of this symbol is obtained by defining for any Gaussian integer
\( \tau \not\equiv 0 \pmod{1 + i} \)

\[
\left( \frac{\alpha}{\tau} \right)_4 = \begin{cases} 
1, & \text{if } \tau \text{ is a unit}, \\
\left( \frac{\alpha}{\pi_1} \right)_4 \cdots \left( \frac{\alpha}{\pi_r} \right)_4, & \text{if } \tau \text{ is not a unit and } \tau = \pi_1 \cdots \pi_r
\end{cases}
\]

where the \( \pi_i \) are primes.

If \( \alpha, \beta, \tau, \rho \) are Gaussian integers with \( \tau, \rho \not\equiv 0 \pmod{1 + i} \) then it is easily
verified that

\[
\left( \frac{\alpha}{\tau} \right)_4 = \begin{cases} 
1, & \text{if } (\alpha, \tau) = 1, \\
\left( \frac{\alpha}{\tau} \right)_4, & \text{if } (\alpha, \tau) \neq 1.
\end{cases}
\]

Received by the editors January 31, 1975.
Key words and phrases. Gaussian integers, biquadratic residues, primary integers, biquadratic
reciprocity.

© American Mathematical Society 1976
(4) \[
\left( \frac{\alpha \beta}{\tau} \right)_4 = \left( \frac{\alpha}{\tau} \right)_4 \left( \frac{\beta}{\tau} \right)_4, \quad \left( \frac{\alpha}{\tau \rho} \right)_4 = \left( \frac{\alpha}{\tau} \right)_4 \left( \frac{\alpha}{\rho} \right)_4,
\]
and

(5) \[
\left( \frac{\alpha}{\tau} \right)_4 = \left( \frac{\beta}{\tau} \right)_4 \quad \text{if} \quad \alpha \equiv \beta \pmod{\tau}.
\]

Also we have

(6) \[
\left( \frac{i}{\tau} \right)_4 = i^{\left( \frac{N(\tau)-1}{4} \right)},
\]
so that in particular if \( k \) is a rational integer \( \equiv 1 \pmod{4} \) then

(7) \[
\left( \frac{i}{k} \right)_4 = (-1)^{\frac{k-1}{4}}.
\]

It is also easy to show that if \( a \) and \( k \) are rational integers with \( (a, k) = 1 \), \( k \) odd, then

(8) \[
\left( \frac{a}{k} \right)_4 = +1.
\]

(See [5, p. 143] for (7) and (8).)

A Gaussian integer \( a + bi \) will be called primary if

\[
a + bi \equiv 1 \pmod{(1 + i)^3},
\]
equivalently \( a + b - 1 \equiv 0 \pmod{4} \) and \( b \equiv 0 \pmod{2} \). A product of primary Gaussian integers is clearly also primary. If a Gaussian integer is not divisible by \( 1 + i \), then among its four associates exactly one is primary. No multiple of \( 1 + i \) can of course be primary. If \( a + bi \) is primary it is convenient to set \( a^* = (-1)^{b^2/2}a \) so that

(9) \[
a^* \equiv 1 \pmod{4}, \quad \frac{a^* - 1}{2} = \frac{a - 1}{2} + \frac{b^2}{4} \pmod{4}.
\]

Also from (6) with \( a + bi \) primary we obtain

(10) \[
\left( \frac{i}{a + bi} \right)_4 = i^{-(a-1)/2}.
\]

We are now in a position to state (see, for example, [3, p. 106])

THE LAW OF BIQUADRATIC RECIPROCITY. If \( \alpha = a + bi, \beta = c + di \) are primary Gaussian integers, then

(11) \[
\left( \frac{\alpha}{\beta} \right)_4 = (-1)^{bd/4} \left( \frac{\beta}{\alpha} \right)_4.
\]

This law was first formulated by Gauss [2] and later proved by Jacobi [4] and Eisenstein [1]. More recently a proof of it has been given by Kaplan [5].
The purpose of this note is to give a simple presentation of the complementary theorem to the law of biquadratic reciprocity relating to the prime 1 + i. The proof uses a special case of (11) namely: if $k$ is a rational integer $\equiv 1 \pmod{4}$ and $\gamma$ is a primary Gaussian integer then

\[(k/\gamma)_4 = (\gamma/k)_4.\]

**Supplement to the law of biquadratic reciprocity.** If $\alpha = c + di$ is a primary Gaussian integer then

\[((1 + i)/\alpha)_4 = i((c+d) - (1+d)^2)/4.\]

(For this formulation see, for example, [6, p. 77].)

**Proof.** We first establish that if $k$ is a rational integer $\equiv 1 \pmod{4}$ then

\[((1 + i)/k)_4 = i((k-1)/4).\]

If $k_1, k_2$ are rational integers $\equiv 1 \pmod{4}$ then

\[\frac{k_1 - 1}{4} + \frac{k_2 - 1}{4} \equiv \frac{k_1k_2 - 1}{4} \pmod{4},\]

so that by (4), as (13) is trivially true when $k = 1$, it suffices to prove (13) for

(i) $k = p$ (prime) $\equiv 1 \pmod{4}$, and (ii) $k = -q$, $q$ (prime) $\equiv 3 \pmod{4}$.

(i) We have $p = \pi\bar{\pi}$, where $\pi, \bar{\pi}$ are primary Gaussian primes, so that

\[\left(\frac{1+i}{p}\right)_4 = \left(\frac{1+i}{\pi}\right)_4 \left(\frac{1+i}{\bar{\pi}}\right)_4 = \left(\frac{1+i}{\pi}\right)_4 \left(\frac{i}{\bar{\pi}}\right)_4 \left(\frac{1-i}{\pi}\right)_4 = \left(\frac{i}{\pi}\right)_4 = i(p-1)/4.\]

(ii) Working modulo $q$ we have

\[\left(\frac{1+i}{-q}\right)_4 = (1+i)(q^2-1)/4 = (2i)(q^2-1)/8 = (2(q-1)/2)(q+1)/4i(q^2-1)/8\]

\[\equiv ((-1)(q^2+1)/4)(q+1)/4i(q^2-1)/8 = (-1)(q+1)/4i(q^2-1)/8\]

\[\equiv i(q+1)/2+(q^2-1)/8 = i(-q-1)/4,\]

so that

\[\left(\frac{(1+i)^2}{-q}\right)_4 = i(q-1)/4.\]

This completes the proof of (13).

Now set $\alpha = c + di = k(a + bi)$, where $(a,b) = 1$ and $k \equiv 1 \pmod{4}$, so that $a + bi$ is primary. Then we have

\[\left(\frac{1+i}{a+bi}\right)_4 = \left(\frac{1+i}{a}\right)_4 \left(\frac{1+i}{b}\right)_4 = \left(\frac{1+i}{a}\right)_4 \left(\frac{i}{b}\right)_4 \left(\frac{1-i}{a}\right)_4 = \left(\frac{i}{b}\right)_4 = i(a-1)/4.\]
\[
\left(\frac{1 + i}{a + bi}\right)_4 = \left(\frac{i}{a^*}\right)_4 \left(\frac{bi}{a^*}\right)_4 \left(\frac{1 + i}{a + bi}\right)_4
\]
(by (3), (8))

\[
= \left(-1\right)^{(a^*-1)/4} \left(\frac{a + bi}{a^*}\right)_4 \left(\frac{1 + i}{a + bi}\right)_4
\]
(by (5), (7))

\[
= \left(-1\right)^{(a^*-1)/4} \left(\frac{a^*}{a + bi}\right)_4 \left(\frac{1 + i}{a + bi}\right)_4
\]
(by (9), (12))

\[
i^{(a^*-1)/2} \left(\frac{i}{a + bi}\right)_4 \left(\frac{a + ai}{a + bi}\right)_4
\]
(by (4))

\[
i^{(a-1)/2+b^2/4+b^2/2} \left(\frac{i(a - b)}{a + bi}\right)_4
\]
(by (5), (9), (10))

\[
i^{3b^2/4} \left(\frac{a - b}{a + bi}\right)_4
\]
(by (10))

\[
i^{b^2/4} \left(\frac{a + bi}{a - b}\right)_4
\]
(by (12))

\[
i^{b^2/4} \left(\frac{b}{a - b}\right)_4 \left(\frac{1 + i}{a - b}\right)_4
\]
(by (4), (5))

\[
i^{b^2/4+(a-b-1)/4}
\]
(by (8), (13))

\[
i^{((a+b)-(1+b)^2)/4},
\]
so that

\[
\left(\frac{1 + i}{\alpha}\right)_4 = \left(\frac{1 + i}{k}\right)_4 \left(\frac{1 + i}{a + bi}\right)_4
\]
(by (4))

\[
i^{(k-1)/4+(a+b-(1+b)^2)/4}
\]
(by (13))

\[
i^{(ka+kb-(1+kb)^2)/4}
\]

\[
i^{(c+d-(1+d)^2)/4}.
\]

REFERENCES


2. C. F. Gauss, (i) Theoria residuorum biquadraticorum. I, Göttinger Abh. 6 (1828);
   (ii) Theoria residuorum biquadraticorum. II, Göttinger Abh. 7 (1832).


